

REMARKS

Applicants appreciate the thorough examination of the present application that is evidenced in the Official Action of August 24, 2005 (the "Official Action"). Applicants have addressed the objections to the specification and claims raised in the Official Action. Claims 1-2, 4, 6-14, 18-20 and 23-26 have been amended as provided in the Listing of Claims. For the reasons discussed below, Applicants submit that the present application is in condition for allowance, which action is respectfully requested.

Status of the Claims

Claims 1-26 are pending in the present application. Claims 1-4, 21-22 and 24-26 stand rejected as unpatentable under 35 U.S.C. § 103(a) over U.S. Publication 2002/0116605 to Berg in view of U.S. Publication 2001/0044904 to Berg et al. Claims 5-17 and 19-23 stand rejected as unpatentable under 35 U.S.C. § 103(a) over Berg in view of Berg et al. and further in view of Mod_SSL manual. Claims 18 and 20 stand rejected as unpatentable under 35 U.S.C. § 103(a) over Berg in view of Berg et al. and further in view of U.S. Patent No. 5,974,549 to Golan.

Objections to the Specification

The examiner noted that the term "TTP" in paragraph [0047] of the publication of the present application (U.S. Publication No. 2003/0105957) appears to be a typographical error. Applicant notes that paragraph [0047] of the publication corresponds to the paragraph beginning at page 16, line 17 and extending to page 17, line 19 of the application as filed. In the application as filed, the term "FTP" appears at page 17, line 4, rather than "TTP" as shown in the publication. Accordingly, the typographical error noted by the examiner appears to have arisen at the USPTO, and no correction of the application as filed appears necessary. Applicant respectfully requests that, to the extent an error exists in any electronic copy of the text of the present application maintained at the USPTO, such error be corrected at the USPTO.

The examiner further objected to the term Transaction Layer Security in the specification. The term has been amended to "Transport Layer Security" as suggested by the Examiner.

Objections to the Claims

The Examiner objected to the use of the term Transaction Layer Security in Claim 23. Claim 23 has been amended to recite "Transport Layer Security" as suggested by the Examiner.

Claim Rejections

Claims 1-4, 21-22 and 24-26 stand rejected as unpatentable under 35 U.S.C. § 103(a) over U.S. Publication 2002/0116605 to M. Berg ("M. Berg") in view of U.S. Publication 2001/0044904 to R. Berg et al. ("R. Berg et al."). The Official Action states that M. Berg discloses a method of improving security processing in a computing network. Official Action, p. 3. However, M. Berg appears to be related to the operation of server farm information processing systems. See M. Berg., para. [0003]. In particular, M. Berg appears to relate to providing for scalability of bandwidth connections to a server farm (M. Berg, para. [0071]) by performing load-balancing of socket application client requests. See, e.g., M. Berg, para. [0099]. While a server farm may require security processing to process secure socket layer (SSL) communications, such processing is handled in the system of M. Berg by an intelligent network interface card (iNIC). See M. Berg, para. [0206]. The iNIC is distinct from the operating system of the server. See M. Berg, Fig. 3. In contrast, Claim 1 recites selectably securing at least one communication of an executing application program using the provided security processing in the operating system kernel.

The Official Action admits that M. Berg does not disclose providing security processing in an operating system kernel or selectably securing at least one communication of an executing application program using the provided security processing in the operating system kernel, as recited in Claim 1. Official Action at 4. In fact, by performing security processing in an iNIC as opposed to an operating system kernel, M. Berg teaches away from the recitations of claim 1.

The Official Action further states that R. Berg et al. disclose providing security processing in an operating system kernel and selectably securing at least one communication using the provided security processing in the operating system kernel. Official Action at 4-5. R. Berg et al. teach a system and method for providing secure communication directly with kernel level components of a system. See, R. Berg et al., Abstract and para. [0003]. Accordingly R.

Berg et al. teach a system and method for providing secure communications with kernel level components 31 in system 11 by an application 35 which may be located locally in system 11 or remotely in system 35. See R. Berg et al., Figure 1A and associated text at para. [0023] and [0026]. Thus, the transport module 27 of R. Berg et al. (which includes the KSOCKS 74) is logically located in the communication path 33 between the remote site and the protected kernel level components 31. See R. Berg et al., para. [0025].

In contrast, embodiments of the present invention provide for securing communications between a local application program and a remotely executing application program using kernel-based security services. Claim 1 has been amended to recite a method of improving security processing in a computing network, comprising selectably securing at least one communication of an executing application program with a remotely executing application program using the provided security processing in the operating system kernel. Similar amendments have been made to Independent Claims 24-26. No new matter has been introduced by these amendments. R. Berg et al. does not teach or suggest selectably securing at least one communication of an executing application program with a remotely executing application program using security processing provided in the operating system kernel. Accordingly, Applicant respectfully submits that Claims 1 and 24-26 are patentable over M. Berg and/or R. Berg et al., either alone or in combination.

Applicant further submits that M. Berg and R. Berg et al. cannot properly be combined in the manner suggested in the Official Action. As noted above, M. Berg teaches a system and method for providing load balancing in a server farm. See M. Berg, para. [0099]. Load balancing in M. Berg is performed by intelligent network interface devices (iNICs), which are associated with servers in the server farm. See M. Berg, para. [0065]. However, the iNICs are distinct from the operating systems of the servers. See M. Berg, Fig. 3 and para. [0094] ("Conventionally, the protocol stack has been part of the OS and has executed in kernel mode. By comparison, in the illustrative embodiments, the iNIC's protocol stack processor executes instructions to perform the protocol stack operations. Accordingly, such operations are offloaded from the OS."). Data packets received at an iNIC may be forwarded to the server associated

with the iNIC or to another server for processing depending on load balancing requirements. See M. Berg, Fig. 4a and para. [0099]-[0106].

On the other hand, R. Berg et al. is directed to providing kernel-level security for communications with kernel-level resources within a system. See R. Berg et al., Abstract and para. [0003]. Performing kernel-level security for communications by the iNICs would presumably require implementing the functionality of the iNICs in the operating system kernel of the associated servers, which would erase the propounded by M. Berg of performing communication processing using separate iNICs, namely, that load balancing and routing are handled separately from the server processing. See M. Berg, para. [0069] ("Conventionally, as discussed hereinabove in connection with FIG. 1a, the protocol stack is part of the OS, and OS overhead is increased in response to processing of more packets, so that fewer CPU cycles remain available for user-level applications. In that situation, individual server efficiency is decreased in response to increases in CPU contention, bus traffic contention, and memory traffic. By comparison, in the illustrative embodiments, the protocol stack is part of the iNIC instead of the OS, so the server farm operates more efficiently in processing client application requests").

Accordingly, a skilled person would not consider combining M. Berg and R. Berg et al. in attempt to provide kernel-based security for application program communications.

With regard to Claim 2, the Official Action states that M. Berg discloses configuring one or more ports used by the provided application program such that communications using the ports are to be secured, and wherein the selectably securing step then secures all communications using the configured ports. Official Action at 6. As noted above, M. Berg relates to load balancing in a server farm. According to M. Berg, when a request packet associated with an SSL connection is received at an iNIC port, the iNIC checks to see if the associated server is the iNIC's server. See M. Berg. para. [0206]. If so, the iNIC performs the suitable operation in response to the request packet. If the associated server is different than the iNIC's server, the iNIC simply outputs the request packet to the associated server's iNIC for performing the suitable operation in response to the request packet. Id. Thus, it appears the receiving iNIC may not perform any security processing for packets that are not destined for the iNIC's server.

Accordingly, M. Berg does not teach that the iNIC selectably secures all communications using a configured port.

With regard to claim 3, the Official Action states that R. Berg et al. disclose wherein the provided application program does not include code for security processing. Official Action at 7. The Official Action asserts that an API call (presumably to the KCMAPI of R. Berg et al.) is required "because the actual code is not within the application." Id.

Claim 3 is dependent from claim 1. Applicant respectfully submits that the discussion of R. Berg et al. at para. [0027] cited in the Official Action relates to communications between a local application 35 and a kernel level service 31 rather than communications between a local application program and a remote application program as recited in claim 1. In any case, assuming that the application program 35 contains commands to issue a KCMAPI call to invoke security processing as asserted in the Official Action, such commands would constitute code within the application program for security processing. As explained in the present application, some embodiments of the present invention provide security processing for applications that are not SSL-enabled (that is, they do not contain code to invoke or perform SSL functions). See Specification, p. 12, ll. 12-13. To the extent R. Berg et al. teaches that security processing functions of the KCMAPI of R. Berg et al. are invoked by API calls from an application program, R. Berg et al. teaches away from the recitations of Claim 3.

With regard to Claim 22, the Official Action states that M. Berg discloses that the provided security processing implements Secure Sockets Layer. Official Action at 9. However, as discussed above, the SSL implementation of M. Berg is performed by the iNICs, which are separate and distinct from the operating system kernel. See M. Berg, Fig. 3 and para. [0094] ("Conventionally, the protocol stack has been part of the OS and has executed in kernel mode. By comparison, in the illustrative embodiments, the iNIC's protocol stack processor executes instructions to perform the protocol stack operations. Accordingly, such operations are offloaded from the OS."). Accordingly, M. Berg teaches away from providing security processing in an operating system kernel wherein the provided security processing implements Secure Sockets Layer as recited in Claim 22.

The remaining dependent claims are patentable at least as per the patentability of Claim 1.

Amendments to the Claims to Address Certain Formalities

Claims 1-2, 4-15, 18-20 and 26 have been amended to provide minor corrections to certain formalities. For example, Claims 1-2, 4, 6-14 and 18-20 have been amended to remove the recitations of "step," and Claim 26 has been amended to replace the recitation of "means for" with "configured to." Claims 2, 5-9, 15 and 26 have been amended to change "one or more" to "at least one." Claims 10, 11, 18 and 19 have been amended to change "includes" to "comprises." No new matter has been introduced by these amendments.

CONCLUSION

In light of the above amendments and remarks, Applicants respectfully submit that the above-entitled application is now in condition for allowance. Favorable reconsideration of this application, as amended, is respectfully requested. If, in the opinion of the Examiner, a telephonic conference would expedite the examination of this matter, the Examiner is invited to call the undersigned attorney at (919) 854-1400.

Respectfully submitted,



David C. Hall
Registration No. 38,904
Attorney for Applicants

Customer Number 46589
Myers Bigel Sibley & Sajovec, P.A.
P.O. Box 37428
Raleigh, NC 27627
919-854-1400
919-854-1401 (Fax)